Explotando un Sistema de Gestión Integrado

Por el Dr. David Brewer MIOD, Dr. Michael Nash FBCS, William List CA, hon. FBCS
[N. del T.: MIOD = Member of the Institute Of Directors; FBCS = Fellow of British Computer Society, CA = Chartered Accountant]

Introducción

En este documento proponemos una estructura para un Sistema de Gestión (SG) integrado y mostramos cómo puede ser aprovechado para ayudar a una organización a lograr su misión mediante el cumplimiento de *todos* los aspectos de sus objetivos de negocio.

La estructura propuesta:

- Satisface los principios de control interno especificados por el Comité de Prácticas de Auditoría ("Audit Practices Board") [1] del Reino Unido;
- Cumple con los requisitos de los estándares ISO para sistemas de gestión.

Comenzamos considerando el modelo Deming para la gestión de procesos y mostramos cómo está implícito, tanto en las recomendaciones del Comité de Prácticas de Auditoría del Reino Unido sobre cómo estructurar un sistema de control interno, como en los requisitos de los estándares ISO de sistemas de gestión.

Posteriormente, explicamos cómo un SG puede implementar el modelo Deming y satisfacer todos los aspectos de los objetivos de negocio de una organización, con el uso de los Planes de Aprovechamiento de Oportunidades (PAOs) y los Planes de Tratamiento del Riesgo (PTRs).

Juntos, los PAOs y los PTRs deberían identificar todos los procedimientos necesarios para que una organización alcance sus objetivos de negocio y sea dirigida con arreglo a sus obligaciones legales, regulatorias, contractuales y de buen gobierno corporativo. Sin embargo, existe una limitación en el modelo de Deming, y es que las omisiones son detectadas únicamente después de tener lugar. Explicamos por qué esto es peligroso y la necesidad, por tanto, de algún otro tipo de análisis de riesgos potenciales, una "Red de Seguridad". Proponemos cómo puede implantarse una, mediante el uso de las "Listas de Ideas Alternativas" (LIAs).

Presentamos un caso de estudio, utilizando un ejemplo de Ventas y Marketing, para ilustrar los conceptos de PAO, PTR y Red de Seguridad y de cómo estos conceptos pueden ser aprovechados en la realización de todos los demás objetivos de negocio.

Finalmente, formulamos nuestras conclusiones.

El modelo de Deming

Tras la publicación del Informe Turnbull (Turnbull Report [2]), el Comité de Prácticas de Auditoría del Reino Unido publicó un conjunto de directivas sobre la estructura de un Sistema de Control Interno (SCI) [1], ver Figura 1.

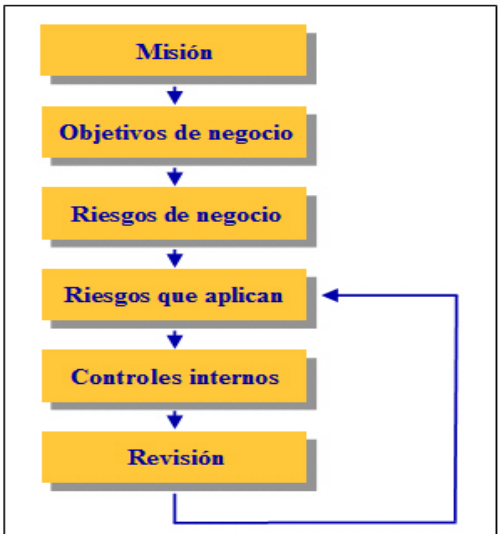

Fig. 1: Modelo APB de control interno
[N. del T.: APB es el *Auditing Practices Board* -Comité de Prácticas de Auditoría- del Reino Unido e Irlanda.]

Como se muestra en la figura, existen actividades asociadas con los controles internos y que, por lo tanto, forman parte del SCI, aunque por sí mismas no constituyan controles internos. Estas actividades (misión, riesgos de negocio, riesgos que aplican y revisión) son los medios para establecer y guiar el SCI. El ciclo de revisión, que busca determinar la efectividad del SCI y actuar en consecuencia, es bien conocido en los círculos ISO como modelo de Deming o ciclo Plan-Do-Check-Act (PDCA):

- PLAN: decida qué quiere hacer;
- DO: hágalo;
- CHECK: determine si funciona bien;
- ACT: actúe en consecuencia.

En la actualidad existen muchos estándares ampliamente aceptados que están basados en el modelo de Deming. Entre ellos hay tres estándares internacionales bien conocidos:

- ISO 9001 [3], que es una especificación de un Sistema de Gestión de la Calidad (SGC);
- ISO 14001 [4], que es una especificación de un Sistema de Gestión Ambiental (SGA).

- ISO/IEC 27001[1] [5], que es una especificación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Todos estos estándares tienen en común un marco explícito PDCA y, por tanto, el modelo de Deming. Además, el proceso requerido por cada uno de estos estándares se corresponde con las directivas para un control interno efectivo del Comité de Prácticas de Auditoría del Reino Unido.

Ahora que estos estándares están afianzados, los Cuerpos de Certificación (es decir, las organizaciones que certifican la conformidad de las empresas con los estándares) abogan por un enfoque integrado, por el cual una organización dispone de un único SG que cumple con varios estándares. El motor principal esta iniciativa es la constatación de que el disponer de SG independientes y, por tanto, cada uno bajo la dirección de equipos gerentes distintos y autónomos, no favorece las buenas prácticas de negocio. Existe un grave peligro de que cada uno tire en distintas direcciones, sin trabajar unidos en busca de un objetivo común. La buena noticia es que tal integración es ciertamente posible [6].

Por eso, tiene sentido basarse en este marco PDCA común al proponer una estructura de SG integrado.

Implementación

Control Interno

Un SCI es la forma en que la dirección despliega los recursos de la organización para lograr los objetivos de la misma. Se compone de dos partes:

- Procedimientos para realizar el trabajo necesario para dirigir la actividad de la organización. Estos se denominan procedimientos operacionales.

- Procedimientos para garantizar que el negocio se dirige según lo esperado. Estos se denominan controles.

PAOs y PTRs

ISO/IEC 27001 reconoce la necesidad de seleccionar controles en base a la capacidad de los mismos de reducir el riesgo a un nivel aceptable. Introduce el concepto de Plan de Tratamiento del Riesgo (PTR) como el medio para seleccionar los controles apropiados, es decir, aquellos que deberían reducir el riesgo hasta un nivel aceptable y no otros.

Los PTRs, sin embargo, sólo tratan la segunda parte de un SCI. Con objeto de tratar la primera parte, hemos ideado el concepto complementario de Plan de Aprovechamiento de Oportunidades (PAO) [7].

Los PTRs vinculan los *eventos* de negocio y los *impactos* adversos, para identificar los controles necesarios que reduzcan el riesgo a un nivel aceptable [8]. Los PAOs vinculan las *oportunidades* de negocio y los *beneficios* de negocio, para crear los procedimientos necesarios para aprovechar las oportunidades de obtener beneficios.

Estructura de SG propuesta

La Figura 2 muestra la estructura propuesta de un SG integrado que hace uso de este marco PDCA común. Se presenta en cuatro cuadrantes, uno por cada fase del ciclo PDCA. Incluye los conceptos de PTR y PAO necesarios para identificar *todos* los controles internos y, por lo tanto, establece un sistema completo de control interno.

Los procedimientos operacionales y controles son identificados en la fase PLAN y puestos en práctica en la fase DO. En las fases CHECK y ACT, la organización evalúa la capacidad de sus controles internos para cumplir con los objetivos de negocio y satisfacer sus obligaciones legales, regulatorias, contractuales y de gobierno.

A excepción de la "red de seguridad", que se trata más adelante, explicamos los componentes de cada cuadrante en las siguientes cuatro secciones.

Plan

Comenzando con la fase PLAN, la primera actividad es una declaración de la misión de la organización. Esta actividad sirve para establecer el contexto general del SCI y conduce a la declaración de los objetivos de negocio de la organización.

Los objetivos de negocio ocasionan:

- Declaraciones de política;

- Riesgos de negocio;

- Oportunidades de negocio.

Un ejemplo de declaración de política sería la famosa cita de Henry Ford "puedes escoger cualquier color de automóvil que te guste, siempre que sea el negro". La declaración impone los procedimientos operacionales y los controles.

Como se sugiere en [1], algunos riesgos, en ausencia de cualquier control interno, pueden ser aceptables. En este caso, el riesgo no es objeto de consideraciones adicionales y es denominado como "riesgo

[1] Este estándar internacional ha reemplazado al extendido estándar SGSI británico BS7799-2.

no-aplicable" [2]. Si, a juicio de la dirección, el riesgo es inaceptable, se le denomina "riesgo aplicable". En este caso, existirá la necesidad de controles internos que reduzcan dicho riesgo hasta un nivel aceptable y éstos serán determinados como resultado de la creación de PTRs.

Las oportunidades de negocio son tratadas de modo similar. En primer lugar, las oportunidades son divididas en aplicables o no. Los procesos operacionales necesarios para aprovechar las oportunidades aplicables se obtienen entonces de los PAOs.

Check

La fase CHECK incluye tres actividades exigidas por el marco común PDCA, que son: la auditoría interna, la revisión por parte de la dirección y el *feedback* del cliente. Adicionalmente, pueden incluirse otras actividades de comprobación, tales como las verificaciones de conciliación rutinarias.

Act

La fase ACT incluye tres actividades exigidas por el marco común PDCA, que son: la acción correctiva, la acción preventiva y la mejora.

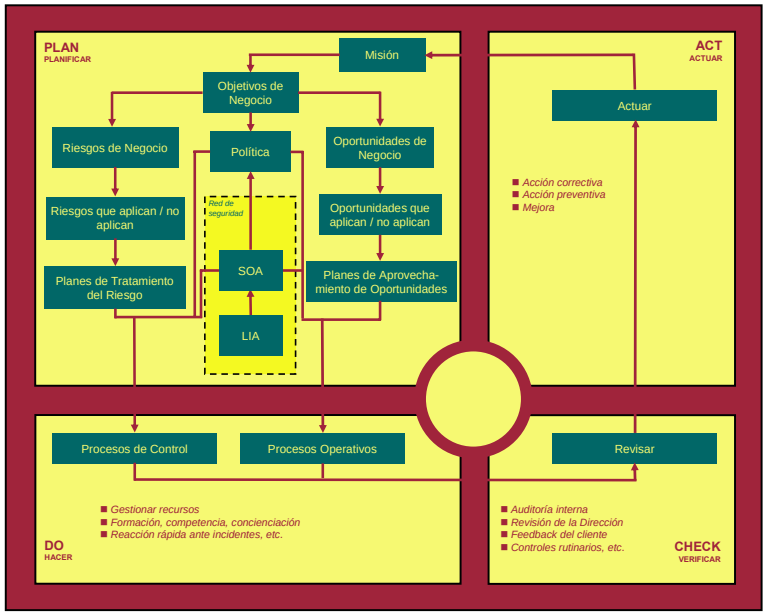

Fig. 2: Estructura del SG integrado

Do

En la fase DO se aplican los procedimientos operacionales y controles. El marco común PDCA requiere una serie de actividades adicionales, como:

- La gestión de los recursos;
- Garantizar que toda la plantilla esté adecuadamente concienciada y formada y sea competente para desempeñar sus responsabilidades;
- Garantizar una reacción inmediata a los incidentes y a las oportunidades.

Limitaciones

Teóricamente, el desarrollo de PAOs y PTRs debería ser suficiente para la identificación de todos los controles internos.

En la práctica, sin embargo, pueden existir errores de omisión debido a que los riesgos y oportunidades no sean correctamente entendidos, especialmente cuando el análisis se efectúa por primera vez durante la fase PLAN del ciclo PDCA. Estos errores deberían ser localizados y corregidos durante las fases Check y Act pero, por supuesto, podría ser demasiado tarde para impedir pérdidas evitables (u oportunidades perdidas) a la organización. Como comprobación adicional de planificación introducimos, por ello, el concepto de "Lista de Ideas Alternativas" (LIA), la cual actúa como una "Red de Seguridad".

La Red de Seguridad

La red de seguridad consiste en una o más Listas de Ideas Alternativas (LIAs).

[2] Aunque es prudente disponer de un PTR para tratar el riesgo que supone el que un riesgo no aplicable llegue a convertirse en un riesgo aplicable.

Una LIA es un conjunto de controles o procedimientos operacionales recomendados. A menudo, se derivan del estudio de las mejores prácticas en alguna materia en particular, tales como seguridad de la información, calidad o finanzas. Un SG puede utilizar tantas LIAs como la dirección desee. Un ejemplo de una LIA es el Anexo A de ISO/IEC 27001. Otro ejemplo son los requisitos para la Realización del Producto (sección 7) de ISO 9001.

Cada control (o procedimiento operacional) incluido en la LIA es revisado para determinar si es aplicable a la organización o no. Se dan tres casos:

- Caso 1: el control (o procedimiento operacional) de la LIA es aplicable y ya había sido identificado en un PTR (o PAO);
- Caso 2: el control (o procedimiento operacional) de la LIA es aplicable pero no había sido identificado en un PTR (o PAO);
- Caso 3: el control (o procedimiento operacional) de la LIA es no-aplicable.

El caso 2 indica que ha existido un error de omisión en el desarrollo de los PTRs (o PAOs). Por lo tanto, la LIA actúa como red de seguridad para las actividades de los PAOs y PTRs.

Una SOA [Declaración de Aplicabilidad] es una LIA en la cual todos los controles (o procedimientos operacionales) han sido declarados como aplicables o no-aplicables.

Observe en la Fig. 2 que hay un enlace entre SOA y Política. Esto es un mecanismo muy práctico, ya que, a menudo es más sencillo introducir un control omitido mediante la creación de una declaración en las políticas, que rehacer los PTRs o los PAOs.

Así pues, la red de seguridad consiste en identificar y crear una o varias Listas de Ideas Alternativas, revisar sus contenidos para comprobar que PTRs y PAOs están realmente completos y, finalmente, crear declaraciones de aplicabilidad (SOAs) asociadas para registrar los resultados de la revisión.

Caso de estudio

Hemos hecho un SG utilizando esta estructura. Está certificado y conforme tanto con ISO 9001 como con ISO/IEC 27001. Esto demuestra que la propuesta de estructura de SG cumple con el Marco Común PDCA. Tiene dos LIAs y SOAs asociadas, una para cada estándar.

Hemos ampliado el SG con la incorporación de dos PTRs y tres PAOs para tratar los riesgos y amenazas asociados con Ventas y Marketing. El primer PTR trata el riesgo de que un producto nicho se transforme en una *commodity* y el segundo trata el riesgo de fracaso en ganar negocio. Los PAOs se describen en [7] y tratan la presencia en el mercado, las encuestas a clientes y la entrega de producto.

Como prueba del concepto de Red de Seguridad, hemos identificado y aplicado una LIA de apoyo al proceso de Ventas y Marketing. La LIA elegida fue el libro de Ries y Trout titulado “Las 22 Leyes Inmutables del Marketing” [9]. Estas “leyes” no constituyen de ninguna manera un estándar, sino que son un conjunto de sugerencias, basadas en la experiencia y observaciones de los autores, relativas a las buenas prácticas del marketing. La elección de [9] refuerza el porqué de denominar a una LIA como Lista de Ideas Alternativas; siendo sugerencias, más que requisitos, las leyes de Ries y Trout son realmente un conjunto de ideas alternativas.

Decidimos que todas las leyes de Ries y Trout eran aplicables a la organización del caso de estudio y trillamos los dos PTRs y los tres PAOs para determinar dónde y de qué manera estaban relacionados con esas leyes. Quizás sin demasiada sorpresa, encontramos que, a pesar que ninguna de las leyes se mencionaba por su nombre, el uso de la mayoría de ellas estaba implícito en los PTRs y PAOs. Existían algunas excepciones, que solucionamos, en general, añadiendo algunas palabras a una PAO, ya que esto se ajustaba mejor al enfoque de ventas y marketing de la organización.

Lo que encontramos sorprendente fue la distribución: 16 leyes referidas a PAOs, mientras que sólo 6 se referían a controles. De no haber existido PAOs, habríamos tenido dificultades para justificar las 16 leyes. Nuestra conclusión es que la mayoría de esas leyes conciernen a “hacer el trabajo”, es decir, la Parte 1 de un SCI. Las otras conciernen a “hacer el trabajo correctamente”, es decir, la Parte 2 de un SCI.

El análisis del documento de Actividad de Ventas y Marketing reveló que, tras los mencionados ajustes del PAO, no había leyes que no hubiesen sido implementadas, pero había instrucciones que no se correspondían, o contradecían, las leyes de Ries y Trout. Estas instrucciones correspondían a los requisitos de los PTRs y PAOs que no figuraban en las leyes de Ries y Trout, pero aun así eran requeridas, no por una cuestión de políticas sino como resultado del análisis de la gerencia de tratamiento del riesgo y aprovechamiento de oportunidades.

Explotación adicional

El Caso de Estudio tal y como se ha descrito cubre Ventas y Marketing, Seguridad de la Información y Calidad. Sin embargo, el SG de la organización del Caso de Estudio también trata las finanzas en cuan-

to a que el crédito y los riesgos en los intercambios comerciales están incluidos en el análisis de riesgos del negocio (fase PLAN), y existen los correspondientes PTRs y procedimientos financieros y controles. Lo que falta, si es que falta algo, es la LIA financiera aparejada. Esta se encuentra actualmente en elaboración.

Resumen y conclusiones

En este documento hemos propuesto una estructura para el sistema de gestión de un SCI. La estructura propuesta:

- Cubre ambas partes de un SCI, mediante el uso de PTRs y PAOs;
- Recoge todas las recomendaciones del modelo de control interno del Comité de Prácticas de Auditoría del Reino Unido;
- Se ajusta al Marco Común PDCA;
- Adopta el concepto de *red de seguridad*, utilizando LIAs y SOAs.

Hemos construido un SG usando la estructura propuesta y lo hemos ampliado para cubrir Ventas y Marketing, mediante la incorporación de 2 PTRs, 3 PAOs y 1 nueva LIA. Esto demostró la facilidad de ampliar un SG estructurado de la forma propuesta.

Utilizamos con éxito un libro de texto para la LIA. Esto demuestra que las LIAs puedan adoptar muchas formas y no necesariamente tienen que ser estándares internacionales formales. El descubrimiento de "leyes" incluidas en la LIA, que eran aplicables pero no estaban referenciadas en ningún PTR o PAO, demuestra la efectividad del concepto de red de seguridad.

El hecho de que los PTRs y PAOs requiriesen una serie de procedimientos operacionales que no estaban relacionados en la LIA refuerza el hecho de que la LIA es simplemente un conjunto de ideas alternativas que no son exhaustivas y que pueden ser o no aplicables. ISO/IEC 27001:2005 realiza una observación similar, indicando que una organización puede requerir de controles adicionales a los especificados en su Anexo A.

Muchas de las ideas en esta LIA en particular se refieren a la Parte 1 de un SCI. Su aplicabilidad no podría haber sido justificada sin la presencia de los PAOs.

Referencias

[1] "*Briefing paper - Providing Assurance on the effectiveness of Internal Control*" publicado en el Audit Practices Board de Julio de 2001. Ver http://www.apb.org.uk. Copias de ABG Professional Information info@abgpublications.co.uk

[2] "*Internal Control, Guidance for directors on the Combined Code*" (The Turnbull Report), Institute of Chartered Accountants de Inglaterra y Gales. Ver http://www.icaew.co.uk/

[3] "*Quality management systems – Requirements*", BS EN ISO 9001:2000

[4] "*Environmental management systems - Specification with guidance for use*", BS EN ISO 14001:1996

[5] "*Information security management systems – Requirements*", BS EN ISO/IEC 27001:2005

[6] "*The Similarity between ISO 9001 and BS 7799-2*", Brewer, D.F.C., Nash, M.J., http://www.gammassl.co.uk/topics/ics/9001Similarities.pdf, Octubre 2005

[7] "*Opportunity Exploitation Plans*", Brewer, D.F.C., List, W., Noviembre 2005, www.gammassl.co.uk/topics/ics/OEP.pdf

[8] "*Measuring the effectiveness of an internal control system*", Brewer, D.F.C., List, W., Marzo 2004, http://ww.gammassl.co.uk/topics/time

[9] "*The 22 immutable laws of marketing*", Ries, A., y Trout, J., HarperCollins, 1994, ISBN 0 00 638345 9

Acerca de los autores

Dr. David Brewer

El Dr. David Brewer está involucrado en seguridad de la información desde que dejó la universidad y es un consultor internacionalmente reconocido en esta materia. Formó parte del equipo que creó ITSEC y los Criterios Comunes y ha trabajado para un gran número de departamentos gubernamentales y empresas tanto en su país como fuera de él. Fue uno de impulsores de los estándares internacionales de SGSI y ha ayudado a muchos clientes en la elaboración de sus SGSIs desde 1998 en Europa, África Oriental, Oriente Medio y Lejano Oriente.

Dr. Michael Nash

El Dr. Michael Nash tiene una amplia experiencia en seguridad de la información. Su primera participación tuvo lugar en 1985, trabajando inicialmente en la OTAN en la utilización del US TCSEC "Orange Book" y, después, estableciendo y gestionando el primer instrumento para la evaluación de la seguridad en el Reino Unido. Colaboró en el desarrollo de un criterio de ámbito nacional en el Reino Unido, el ITSEC y, finalmente, los Criterios Comunes. Por otro lado, ha asesorado a muchas grandes empresas y organizaciones de usuarios en cómo implantar y mejorar la seguridad de la información, mediante el uso de BS 7799 y técnicas relacionadas. Ha estado implicado en la estandarización internacional durante más de quince años y, más recientemente, como editor del proyecto para la "Guide to the Development of Protection Profiles and Security Targets, ISO/IEC TR 15292".

William List, CA. hon FCBS, CITP

William List, CA hon FBCS CITP, es el propietario de W^{m}. List & Co. Ha estado involucrado en temas de seguridad y auditoría desde hace unos 40 años. Ha participado en el desarrollo de aplicaciones de negocio seguras y el desarrollo de varios estándares de contabilidad y TI. Forma parte, también, del equipo internacional que desarrolla los estándares internacionales de SGSI. Se jubiló como socio de KPMG. Fue el anterior presidente del foro de expertos de seguridad de BCS.

[Traducción del original inglés por Agustín López Neira, www.iso27000.es]
[Translated from English original by Agustín López Neira, www.iso27000.es]